UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF RHODE ISLAND

UNITED STATES OF AMERICA	)	
v.	)	Cr. No. 21-120
JAMES WARD JACKSON,	)	
Defendant.	)	

MEMORANDUM AND ORDER

WILLIAM E. SMITH, District Judge.

Defendant James Ward Jackson is charged with one count of receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2) and one count of possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). See Indictment, ECF No. 14. He now moves to suppress evidence obtained from the search of multiple buildings at St. Mary's Catholic Parish in Providence, Rhode Island, arguing that the warrant did not describe with adequate particularity the place to be searched or the things to be seized. For the reasons that follow, the Motion to Suppress, ECF No. 36, is DENIED.

I. Background

On September 4, 2021, Detective Corporal Stephen Evans of the East Providence Police Department, a member of the Rhode Island State Police Internet Crimes Against Children Task Force, observed

that a device connected to a particular Internet Protocol ("IP") address in Providence was sharing files of suspected child pornography on a file-sharing network. Def.'s Mem. Supp. Mot. Suppress ("Def.'s Mot. Suppress") 1-2, ECF No. 36-1. Detective Evans viewed some of the seventy-one files and believed that they were consistent with the definition of child pornography contained in R.I. Gen. Laws § 11-9-1.3. Def.'s Mot. Suppress 2.

Detective Evans sent legal process to the internet servicer, Verizon Fios, which responded that the subscriber to the IP address was St. Mary's Church in Providence, Rhode Island. Id. Detective Evans went to the church and observed that there were two buildings at that address: a stone church with a sign reading "St. Mary's Catholic Parish" and a yellow rectory next to the church, housing the church's offices, the priests' living spaces, and storage areas. Id. He was able to see the locked WiFi network and determined that anyone within about 150 feet of the WiFi router could access the network if they had the password, which is consistent with the broadcast range of a typical router. Id.

Thereafter, Detective Evans was notified that a device using the IP address assigned to the church accessed a file-sharing network again on September 26, October 15, and October 17, all outside of church activity hours. Id. The October 15 connection revealed nine files, several of which Detective Evans believed were consistent with the definition of child pornography. Id. at

2-3.

Detective Evans applied for a search warrant, providing the following description of the things to be seized:

> Computer hardware, computer software, mobile devices, and portable digital storage devices, to include the contents therein. Additionally, any and all computer-related documentation, records, documents, materials, proceeds, passwords or other data security devices related to the possession and transfer of child pornography. Refer to Attachments "A" and "B" attached hereto and made a part hereof.

Def.'s Mot. Suppress Ex. 1 ("Ex. 1") at 1, ECF No. 36-2. Attachment A defined the terms "computer hardware," "computer software," "computer-related documentation," "records, documents, and materials," and "passwords and other data security services." Id. at 10-11. Attachment B explained that, due to the "volume of evidence" and the "technical requirements" for searching it, "which can take weeks or months," the items listed would be seized and the contents would be searched thereafter. Id. at 12-14.

Detective Evans also described the place to be searched:

> The premises located at 538 Broadway, Providence, Rhode Island 02909. Said premises is described as a stone church with "St. Mary's Catholic Parish" affixed to a sign in the front of the building. The search will include exterior buildings on the property to include the detached yellow building commonly known as the rectory. The search will include storage spaces located on the premises used by residents.

Id. at 1.

Law enforcement agents executed the search warrant. Aff. Supp. Compl. ¶ 6, ECF No. 3-1. They seized an external hard drive

from Defendant's office area in the rectory, which adjoined his bedroom. Id. ¶ 7. A search of the hard drive revealed hundreds of image and video files of child pornography, prompting Defendant's arrest. Id.

II. Discussion

A. Particularity

The Fourth Amendment to the United States Constitution states that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV (emphasis added).

> The manifest purpose of [the] particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.

Maryland v. Garrison, 480 U.S. 79, 84 (1987). The particularity requirement also "assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search." United States v. Chadwick, 433 U.S. 1, 9 (1977) (quoting Camara v. Mun. Ct. of City and Cnty. of S.F., 387 U.S. 523, 532 (1967)). "The uniformly applied rule is that a search conducted pursuant to a warrant that fails to conform to the particularity

requirement of the Fourth Amendment is unconstitutional." Massachusetts v. Sheppard, 468 U.S. 981, 988 n.5 (1984).

1. Things to be Seized

Defendant contends that the things to be seized were not sufficiently particularized in the warrant because it "lists a smorgasbord of every conceivable electronic device imaginable" and the government made no effort to narrow the objects of the search. Def.'s Mot. Suppress 12. This argument is unavailing.

"While courts 'have struggled to adapt the Fourth Amendment search doctrines designed for physical spaces to digital contexts,' courts generally recognize that search warrants may authorize broad searches of electronic data on cellphones and computers, without violating the particularity requirement." United States v. Reese, No. 19-cr-257-NR, 2021 WL 4429429 at *4 (W.D. Pa. Sept. 27, 2021) (quoting United States v. Perez, 712 F. Appx. 136, 139 (3d Cir. 2017)); see United States v. Grimmett, 439 F.3d 1263, 1270 (10th Cir. 2006) (warrant authorizing seizure of "[a]ny and all computer hardware," and "[a]ny and all computer software" was not overbroad). This is so because often "agents could not have known which device a defendant used to engage in the conduct relevant to the search," so warrants "'broadly authoriz[e] the seizure of any computers, cell phones, and/or electronic media that could have been used as a means to commit' the described offenses." United States v. Andrade, No. 18-cr-145-

JJM, 2022 WL 179341 at *3 n.7 (D.R.I. Jan. 20, 2022) (quoting United States v. Smith, No. 19-cr-324-BAH, 2021 WL 2982144 at *7 (D.D.C. July 15, 2021)); see United States v. McLellan, 792 F.3d 200, 213-14 (upholding search of devices of three roommates living in shared dwelling because "every internet connection established from any of the occupants' computers would trace back to the same IP address"); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (warrant was not overbroad because "[a]s a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images"). Courts do, however, typically require "sufficiently particularized language creating a nexus with the crime[s] to be investigated." United States v. Loera, 59 F. Supp. 3d 1089, 1151 (D.N.M. 2014) (quoting United States v. Burgess, 576 F.3d 1078, 1091 (10th Cir. 2009)).

Here, the warrant broadly authorized the seizure of devices including "[c]omputer hardware, computer software, mobile devices, . . . portable digital storage devices, . . . and all computer-related documentation, records, documents, material, proceeds, and passwords or other data security devices," which is comparable to the broad authorization to seize electronic devices that other courts have upheld. Ex. 1 at 1; see McLellan, 792 F.3d at 213-14; Grimmett, 439 F.3d at 1270. It also specified that these items must be "related to the possession and transfer of child

pornography," creating the requisite nexus with the crime charged. Ex. 1 at 1; see Loera, 59 F. Supp. 3d at 1151. Therefore, the warrant described the items to be seized with adequate particularity.

2. Place to be Searched

Defendant relies primarily on a series of cases concerning searches of multi-unit dwellings to support his argument that the place to be searched was also not stated with sufficient particularity. See Def.'s Mot. Suppress 5-9. In sum, the Supreme Court and Circuit Courts have held in these cases that "a search warrant directed against an apartment house will usually be held invalid if it fails to describe the particular apartment to be searched with sufficient definiteness to preclude a search of other units located in the building and occupied by innocent persons." United States v. Bedford, 519 F.2d 650, 654-55 (3d Cir. 1975); see also Garrison, 480 U.S. at 85 ("[I]f the officers had known, or even if they should have known, that there were two separate dwelling units on the third floor . . ., they would have been obligated to exclude respondent's apartment from the scope of the requested warrant."); United States v. Votteller, 544 F.2d 1355, 1362, 1364 (6th Cir. 1976) (search warrant describing entire three-floor, multi-use building as place to be searched was insufficiently particular); United States v. Higgins, 428 F.2d 232, 234-35 (7th Cir. 1970) (warrant authorizing search of

"basement apartment" in building that had three basement units was insufficiently particular); United States v. Hinton, 219 F.2d 324, 325 (7th Cir. 1955) ("For purposes of satisfying the Fourth Amendment, searching two or more apartments in the same building is no different than searching two or more completely separate houses. Probable cause must be shown for searching each house or, in this case, each apartment."); Tynan v. United States, 297 F. 177, 179 (9th Cir. 1924) ("No doubt a general search warrant for an entire building, . . . occupied by different families or different tenants, is ordinarily null and void.").

The government argues that the facts of this case are more akin to those cases involving a single premises containing multiple occupants, Gov.'s Opp. Def.'s Mot. Suppress ("Gov.'s Opp.") 5-7, ECF No. 39, in which courts have concluded that "probable cause often exists to search the entire dwelling because it is reasonable to assume the suspect has access to the entire dwelling." United States v. Schwinn, 376 Fed. Appx. 974, 982 (11th Cir. 2010); see also McLellan, 792 F.3d at 212 (while "a warrant that authorizes the search of an undisclosed multi-unit dwelling is invalid," "[a] warrant for a single-unit residence authorizes the search of the entire dwelling regardless of who the area searched belongs to, so long as the items delineated in the warrant could reasonably be found in the searched area"); Durham v. McElynn, 254 Fed. Appx. 892, 896 (3d Cir. 2007) ("While [defendant] may have had a

roommate, this does not convert his single-family home into an apartment house or multi-unit building."); United States v. Ayers, 924 F.2d 1468, 1480 (9th Cir. 1991) (concluding that search of entirety of multi-occupant premises was valid notwithstanding warrant issued based on alleged illegal activities of only one occupant); United States v. Hinds, 856 F.2d 438, 441 (1st Cir. 1988) ("We do not think the mere presence of more than one family in a building automatically changes its character from a single family to a multi-family.").

Courts have highlighted certain hallmarks that distinguish single-family dwellings from multi-unit dwellings. For example, the First Circuit concluded in McLellan that because the defendant's rented room in the searched residence was "not equipped for independent living," did not have its own entrance from the street, and because the defendant shared a common kitchen and living area with the other occupants, the district court properly characterized it as a single-family residence, and therefore the defendant's reliance on cases concerning multi-unit dwellings was misplaced. McLellan, 792 F.3d at 213; see also United States v. Ferreras, 192 F.3d 5, 11 (1st Cir. 1999) (search of attic was permissible under warrant for building's second floor living quarters because it was connected to second floor, did not have separate entrance, and was "not equipped for independent living"). In addition, where "[t]here [a]re no indications, such as separate

doorbells or mailboxes, that more than one family live[s]" in a building, it may be best characterized as a single-family dwelling. Hinds, 856 F.2d at 441-42.

The limitations of the record in the present case make difficult the determination of which of the preceding paradigms is applicable here. Both parties and the search warrant itself refer to the fact that multiple people live and work within the rectory and that it contains storage areas. Def.'s Mot. Suppress 9; Gov.'s Opp. 3; Ex. 1 at 1. The affidavit accompanying the Complaint notes that Defendant had a bedroom and an adjoining office and references a "dining room/common area." Aff. Supp. Compl. ¶ 6. A more detailed description of the building, however, is not provided. From these descriptions, it seems that the rectory does not possess the hallmarks of multi-unit dwellings such as a separate entrance, separate doorbell or mailboxe, and independent living space, and would be best characterized as a single-family residence, making the description in the warrant sufficiently particular, but this cannot be conclusively determined based on the available information.

3. Good Faith Exception

Even assuming that the warrant lacked sufficient particularity in its description of the place to be searched, however, there is no basis for suppressing the evidence because the officers acted in good faith on the judge's determination that

the warrant was sufficient. Under the good faith exception to the exclusionary rule, when police act in "objectively reasonable reliance on a subsequently invalidated search warrant" signed by a neutral and detached magistrate, "the marginal or nonexistent benefits produced by suppressing evidence . . . cannot justify the substantial costs of exclusion." United States v. Leon, 468 U.S. 897, 922 (1984). Where "an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope . . . . there is no police illegality and thus nothing to deter." Id. at 920-21. Thus, "[t]o trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." Herring v. United States, 555 U.S. 135, 144 (2009).

Here, "the warrant, read comprehensively and in context, was not so 'facially deficient . . . that the executing officers [could not] reasonably presume it to be valid.'" United States v. Kuc, 737 F.3d 129, 134 (1st Cir. 2013) (quoting Leon, 468 U.S. at 923)); cf. Sheppard, 468 U.S. at 988, 988 n.5 (officers reasonably relied on validity of warrant even where "the description in the warrant was completely inaccurate and the warrant did not incorporate the description contained in the affidavit"). Neither has Defendant pointed to any misconduct by police here that should be deterred.

Rather, the police did precisely what the Supreme Court has instructed in light of the strong preference for searches conducted pursuant to warrants under the Fourth Amendment. See Illinois v. Gates, 462 U.S. 213, 236 (1983) ("[T]he possession of a warrant by officers conducting an arrest or search greatly reduces the perception of unlawful or intrusive police conduct, by assuring 'the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search.'" (quoting Chadwick, 433 U.S. at 9)). Therefore, even if the warrant was deficient in its description of the place to be searched, the exclusionary rule is not triggered because the officers acted in good faith reliance on the warrant.

B. Regulation

Finally, Defendant calls for "regulation of searches that do not particularly describe the location to be searched or the thing to be seized when dealing with multiple buildings, residents, and employees and multiple potential devices containing massive amounts of digital information." Def.'s Mot. Suppress 15. Analogizing to cases involving wiretapping and cell-site location information, see Carpenter v. United States, 138 S. Ct. 2206 (2018); Katz v. United States, 389 U.S. 347 (1967), where legislatures and courts have limited the scope of permissible searches, Defendant posits that in cases like this, where there

are many possible individuals and devices that could have accessed the illicit material, there should be a similar circumscription. Def.'s Mot. Suppress 15. For example, where the government has shown probable cause that a crime was committed and linked to a particular IP address but has also made a preliminary showing that there is no way to narrow down the search and seizure to make it less intrusive than to seize all devices in the residence, the government could be required to first seize the router associated with the IP address in order to determine which devices were connected at the time the illicit material was accessed. Id. (citing United States v. Stanley, 753 F.3d 114, 115-17 (3d Cir. 2014) (describing how wireless Internet router keeps log of devices that have connected to it), cert. denied, 135 S. Ct. 507).

Defendant's point is well taken. Courts have expressed concern with the search and seizure of electronic devices and have indicated a need for greater restrictions. "Because electronic devices could contain vast quantities of intermingled information, raising the risks inherent in over-seizing data, law enforcement and judicial officers must be especially cognizant of privacy risks when drafting and executing search warrants for electronic evidence," lest such evidence "become a vehicle for the government to gain access to a larger pool of data that it has no probable cause to collect." United States v. Schesso, 730 F.3d 1040, 1042 (9th Cir. 2013) (citation omitted). While this subset of search

and seizure cases may be due for its own Carpenter-like reckoning to account for the evolution of our use of technology and the ever-increasing quantities of personal data stored on our devices, the law as it stands today permits the search that was executed here. In any event, such restrictions would not have helped Defendant in this case, since examination of the router would likely have led the officers right back to Defendant's devices.

III. Conclusion

For the foregoing reasons, Defendant's Motion to Suppress, ECF No. 36, is DENIED.

IT IS SO ORDERED.

William E. Smith
District Judge
Date: November 14, 2022